**문제 1**

**문항 1. 디지털 포렌식 종류를 서술하시오. (20점)**

**컴퓨터 법과학: USB 드라이브, SD 드라이브 등등 복원**

**모바일 장치 법과학: 내장된 GPS / 위치 추적 또는 셀 사이트 로그 범위 추적, 내장된 통신 시스템(예: GSM)**

**네트워크 법과학: 정보 수집 및 로컬 및 WAN/인터넷의 네트워크 트래픽을 모니터링하고 분석 패킷 레벨 분석법**

**데이터 분석 법과학: 금융 범죄로 인한 사기 행위 패턴을 발견 분석 구조화된 데이터 조사**

**데이터베이스 법과학: 데이터베이스와 관련된 포렌식 / 인로그, 데이터베이스 내용. RAM의 타임라인 구축 및 복구**

 **문항 2. 디지털 포렌식 대상물의 특징을 서술하시오. (30점)**

**

문항 3. 디지털 포렌식 5대 원칙을 서술하시오. (50점)**

1. **정당성의 원칙-**

**획득한 증거 자료가 적법한 절차를 준수해야 하며, 위법한 방법으로 수집된 증거는 법적 효력을 상실한다.**

**2) 독수 독과이론- 위법하게 수집된 증거(독수)에 의하여 발견된 제2차 증거(독과)의 증거능력은 인정할 수 없다는 이론**

**2. 무결성의 원칙-**

**수집 증거가 위, 변조되지 않았음을 증멸할 수 있어야 한다.**

**일반적으로 수집 당시의 데이터 hash 값과 법정 제출 시점 데이터의 hash 값이 같다면 hash 함수의 특성에 따라 무결성을 입증이를 입증하기위해 경우에 따라서 현장에 입장하는 시점부터 조사가 끝나는 시점까지 동영상으로 촬영하거나 사진으로 찍어두는 경우도 있음※ 해시(hash) 함수란? (참고, MD5의 경우 128bit, SHA-1의 경우 160bit로 출력됨)- 평문을 해시 알고리즘을 통하여 해시값으로 출력하는 것특정한 키를 사용하지 않기 때문에 동일한 문장에 대해 동일한 해시값으로 출력하며, 문장이 조금만 변해도 해시값이 달라지게 됨. 또한 해시함수의 종류에 따라 출력되는 해시값의 길이가 달라짐예컨대, '포렌식'의 해시값이 '155F01'라면 '포 렌식'의 해시값은 '14A3E5'으로 약간의 변화에도 완전 다른 해시값이 출력됨**

1. **재현의 원칙-**

**피해 직전과 같은 조건에서 현장 검증을 실시하거나, 재판이나 법정의 검증과정에서도 동일한 결과가 나와야한다. 예컨대, 불법 해킹 용의자의 해킹 툴이 증거능력을 가지기 위해서는 같은 상황의 피해시스템에 툴을 적용할 경우 피해 결과와 일치하는 결과가 나와야한다.**

**4. 신속성의 원칙-**

**휘발성 증거의 수집 여부는 신속한 조치에 의해 결정되므로 모든 과정은 지체없이 진행되야한다.**

**5. 절차 연속성의 원칙** **–**

**증거물 획득 -> 이송 -> 분석 -> 보관 -> 법정 제출의 각 단계에서 담당자 및 책임자를 명확히 해야한다.- 수집된 저장매체가 이동단계에서 물리적 손상이 발생하였다면, 이동 담당자는 이를 확인하고 해당 내용을 정확히 인수 인계하여 이후의 단계에서 적절한 조치가 취해지도록 해야한다.**